



Thomas H. Lenhard

Datensicherheit

Technische und organisatorische
Schutzmaßnahmen gegen
Datenverlust und Computerkriminalität

2. Auflage

EBOOK INSIDE



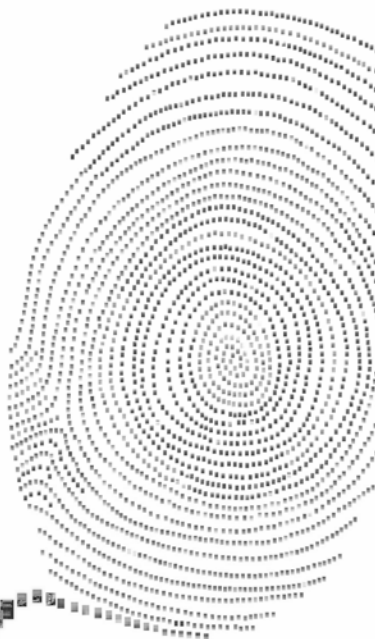
Springer Vieweg

Datensicherheit

Lizenz zum Wissen.

Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf www.springerprofessional.de/buchaktion/



**Jetzt
30 Tage
testen!**

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

-  Zugriff auf tausende von Fachbüchern und Fachzeitschriften
-  Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
-  Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

 Springer

Thomas H. Lenhard

Datensicherheit

Technische und organisatorische
Schutzmaßnahmen gegen Datenverlust
und Computerkriminalität

2., erweiterte und aktualisierte Auflage

 **Springer** Vieweg

Thomas H. Lenhard
Comenius Universität
Bratislava, Slowakei

ISBN 978-3-658-29865-4 ISBN 978-3-658-29866-1 (eBook)
<https://doi.org/10.1007/978-3-658-29866-1>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2017, 2020

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Inhaltsverzeichnis

1	Einleitung	1
2	Datenschutz und Datensicherheit	3
3	Wie Computer miteinander kommunizieren	5
4	Was kann mit Daten geschehen?	15
5	Gefahren im technischen Umfeld	17
6	Gefährliche Software	27
6.1	Das Trojanische Pferd	29
6.2	Der Virus	34
6.3	Die logische Bombe	37
6.4	Der Keylogger	38
6.5	Der Sniffer	39
6.6	Die Hintertür	43
7	Wechseldatenträger, USB-Geräte, Smartphones und andere mobile Geräte	45
8	Telefonsysteme	49
9	Die größte Gefahr in einer digitalisierten Welt	55
10	Zerstörung von Daten	59
11	Datensicherung und Wiederherstellung von Daten	65
12	Verschlüsselung	69

13 Hacken von Webseiten	75
14 Häufige Sicherheitsprobleme	79
14.1 Arbeitskonsolen, die nicht gesperrt werden	79
14.2 Druckerstationen und Multifunktionsgeräte	80
14.3 Arbeiten mit Administratorrechten	80
14.4 Das Internet der Dinge und industrielle Steuerungsanlagen	81
15 Identifizierung von Computern und IP-Adressen	83
16 Die Firewall	87
17 Der Router	91
18 Konfiguration von Schutzsystemen	95
19 Die Demilitarisierte Zone	103
20 Organisatorische Datensicherheit	109
21 Merksätze	111
Schlusswort	115
Literatur	117
Stichwortverzeichnis	119

Abkürzungsverzeichnis

Cat-7	Cable Category 7
CCC	Chaos Computer Club
CTI	Computer Telephony Integration
DBMS	Data Base Management System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarisierte Zone
DNS	Domain Name Service
EN 50173-1	European Normative 50173-1:2011 about Information technology – Generic cabling systems – Part 1: General requirements
ERP	Enterprise Resource Planning
FTP	File Transport Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISO	International Organization for Standardization
LLC	Logical Link Control
MAC	Media Access Control
NAS	Network Attached Storage
NTFS	New Technology File System
NTP	Network Time Protocol
PBX	Private Branch Exchange (Telefonanlage)
PGP	Pretty Good Privacy
POP	Post Office Protocol
RFID	Radio Frequency Identification

RJ45	Registered Jack 45
SFTP	Secure File Transport Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transaction Control Protocol
Telnet (TNP)	Telecommunication Network Protocol
TLS	Transport Layer Security
UNC	Uniform Naming Convention
USB	Universal Serial Bus
USV	Unterbrechungsfreie Stromversorgung
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual Private Network

Abbildungsverzeichnis

Abb. 3.1	Das OSI-Schichtenmodell.	7
Abb. 3.2	Zusatzinformationen im Adressfeld des Browsers	12
Abb. 3.3	Ping	13
Abb. 5.1	Ein Serverschrank im tiefsten Keller des Gebäudes	18
Abb. 5.2	Eine Stahlwanne zum Schutz von IT-Anlagen vor Rohrleitungen . . .	20
Abb. 5.3	Chaos in einem Teil eines klinischen „Rechenzentrums“.	22
Abb. 6.1	Wireshark bei der Analyse von Datenbankabfragen.	40
Abb. 8.1	Trennung von IT- und Telefonnetzwerk	52
Abb. 10.1	Kaliber .44 Magnum und andere kreative Ideen eignen sich nicht als sichere Methode der Datenvernichtung	62
Abb. 19.1	Positionierung eines DMZ-Netzwerks	104

Tabellenverzeichnis

Tab. 3.1 Dienste und Portnummern11

Einleitung

1

Zusammenfassung

Datensicherheit ist ein untrennbarer Bestandteil des Datenschutzes. Während Datenschutz durch nationale oder internationale Gesetze definiert wird und damit weltweit größten Unterschieden unterworfen ist, wird nahezu überall auf der Welt die gleiche Technik eingesetzt, so dass damit zu rechnen ist, dass sich Probleme der Datensicherheit überall auf der Welt zumindest ähneln. Die Einleitung zu dieser Publikation geht hier besonders auf den Umstand ein, dass ein weltweites Netzwerk auch grenzüberschreitende Probleme und Herausforderungen mit sich bringt.

Das Datenschutzrecht unterscheidet sich von Nation zu Nation und variiert manchmal sogar innerhalb einer Nation von Region (Bundesland, Kanton, Departement etc.) zu Region. In einer globalisierten Welt mit einem fast uneingeschränkten Datenverkehr über das Internet enden Aktivitäten und kriminelle Taten allerdings an keiner nationalen Grenze. Natürlich gibt es hierbei auch Ausnahmen: In einigen Staaten, in denen Konzepte wie Freiheit oder Menschenrechte anders interpretiert werden als in der restlichen Welt, muss mitunter mit Einschränkungen im Internet und im freien Zugang zu Informationen gerechnet werden. Die vorliegende Publikation befasst sich mit grundlegenden Fragen der Datensicherheit. Daher werden politische Standpunkte und Anschauungen hier nicht diskutiert. Während gesetzliche Regelungen in unterschiedlichen Nationen oder Bundesstaaten dieser Welt

sich zum Teil elementar unterscheiden, verwenden wir täglich dieselben Betriebssysteme, dieselben Servertypen, dieselbe Hardware, gleiche Notebooks, Drucker und andere EDV-Anlagen. Und das vollkommen unabhängig vom Land, in dem wir leben oder arbeiten. In jenem Moment, in dem diese Zeilen geschrieben werden, ist es möglich, dass Kriminelle von irgendwo auf der Welt versuchen, den Computer des Autors, der sich momentan in Deutschland befindet, anzugreifen. Das Internet macht es möglich, Millionen von Computern weltweit anzugreifen, während der Angreifer bequem zu Hause in seinem Wohnzimmer sitzt.

Im Kontext dieser Publikation verstehen wir das Internet als unbegrenztes, weltweites Netzwerk mit hohem Gefährdungspotential. Ein solches Netzwerk war nur aufgrund technischer Standards realisierbar. Der Umstand, dass wir weltweit anerkannte und verwendete Kommunikationsstandards nutzen, um Dateien, Nachrichten und Informationen über das Internet von einem Ende der Welt zum anderen zu transportieren, sowie die allgegenwärtigen Bedrohungen im Rahmen der Internetnutzung, resultieren bei tieferer Betrachtung der Gesamtsituation in einem Axiom, das den Betrachtungen dieser Publikation zugrunde liegen soll:

Maßnahmen der Datensicherheit sind weltweit in identischer Form umsetzbar.

Aber selbst wenn technische Methoden – theoretisch – überall in der Welt verwendet werden können, möchte der Autor dieses Buches, dass Sie keinesfalls in Konflikt mit nationalem oder lokalem Recht geraten. Also: Denken Sie bitte daran, dass der Gebrauch von einigen technischen Methoden, Geräten oder auch von bestimmter Software in Ihrem Land gesetzlich verboten oder beschränkt sein könnte. Es gibt derzeit viele Staaten weltweit, die gesetzliche Einschränkungen kennen, wenn es zum Beispiel um die Verwendung von Kryptographie und Verschlüsselungssystemen geht. An dieser Stelle soll allerdings schon darauf hingewiesen werden, dass Gefahren für Daten und Systeme nicht nur im Internet lauern.

In den folgenden Kapiteln werden die Grundlagen der Computertechnik erläutert, die notwendig sind, um das Ausmaß und die Gefahr von Internetkriminalität zu verstehen. Insbesondere werden auch sonstige Gefahren im Hinblick auf die Datensicherheit beschrieben und es werden Lösungsansätze vorgestellt, wie Systeme gesichert werden können.